Шакиров Арслан Айнурович,

студент 2-го курса;

Зарипова Римма Солтановна,

канд. техн. наук, доцент,

ФГБОУ ВО «Казанский государственный энергетический университет»,

г. Казань, Республика Татарстан, Россия

ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА В УСЛОВИЯХ ИНФОРМАЦИОННОЙ ВОЙНЫ

В дни открытого доступа к огромному объему информации борьба стала вестись и в информационной области. В данной статье рассматриваются основные источники угроз безопасности личности, общества и государства в условиях информационной войны.

Ключевые слова: информация, информационная безопасность, информационная война, источники угроз информационной безопасности.

Научно-технический прогресс в сфере информационных технологий сформировал невиданные ранее возможности для сдерживания врага при помощи неординарных возможностей поражения, не приводящих к физическим разрушениям. Передавая обществу нужные новости и материалы, можно иметь власть над сознанием большинства населения. Это информационная война.

Понятие информационной войны рассматривается в двух аспектах.

1. Информационное влияние на человека, через распространение верной или ложной информации. Данный вид основан на агитации и пропаганде.

2. Защита собственных информационных систем и атаки на системы соперника. Этот вид связан с физическим воздействием на носители данных. Пример данного вида – кибератаки [1].

Министр третьего рейха Йозеф Геббельс изобрел новый способ информационной войны, основанный на внедрении ложных данных в достоверную информацию. Следовательно, при таких обстоятельствах ложь, связанная с правдой, понималась как правда. Вскоре человечество осознало новую истину: «слово – это самое сильное оружие во всём мире». Поэтому новый вид войны с применением дезинформации, пропаганды и агитации

принято обозначать как информационную войну. В настоящее время всё человечество является свидетелем информационной войны, проводимой государствами.

Ещё один источник угрозы – это кибервойны. Интернет на сегодняшний день имеет всемирную известность. Невозможно представить себе хоть одного человека, который не знал бы ничего об интернете. Сегодня практически у каждой государственной структуры есть свои веб-сайты [2]. Банки практически полностью смогли интегрироваться в интернете, предоставляя клиентам возможность использования своих услуг даже с мобильного телефона [3]. Именно данная интеграция со «всемирной паутиной» и таит опасность.

Российские сайты по предоставлению услуг не распространены в народе, а поэтому их и атакуют нечасто. А вот европейские и американские веб-сайты, дающие возможность пользования госуслугами, при атаке на них могут потерять огромные средства. Существуют несколько держав, чьи взаимные кибератаки уже стали частью истории. Количество взломанных сайтов этих государств уже давно преодолело порог в тысячу. Самый элементарный способ взломать сайт – это совершить против него DDOS атаку (DDOS – denial of service – отказ в обслуживании). Сущность такой атаки состоит в том, что хакеры посылают на веб-сайт массу бессодержательных запросов. Вследствие чего сайт не выносит такой нагрузки и прекращает свою работу.

Гибридной формой информационной борьбы являются сетевые войны. В них элементы медиа-войн и кибервойны смешиваются, размещаясь на информационной площадке межнациональных сетей. С одной стороны, через инфраструктуру платформ (например, Фэйсбук или Твиттер) людям транслируются и внедряются картины мира, которые создаются большими масс-медиа. С другой стороны, соцсети служат для несогласованного получения секретной базы. Соцсети играют главную роль и в общественно-политических действиях, что ярко показал опыт компании Фэйсбук, которая стала одним из решающих феноменов «арабской весны». Соцсети являются проводником любой псевдоинформации, могут дать ей статус правдивой и

вызвать негативный резонанс. Люди, которые не имеют возможности получать достоверную информацию, находятся в состоянии паники, стресса, апатии, снижается их трудоспособность. Следовательно, в условиях информационной войны обеспечение информационно-психологической безопасности граждан является одной из основных задач государства.

СПИСОК ЛИТЕРАТУРЫ

1. Бикмухаметов И.И. Кибертерроризм как угроза информационной безопасности / И.И. Бикмухаметов, Р.С. Зарипова // Аллея науки. – 2018. – Т.1. – №2(18). – С. 266-268.

2. Злыгостев Д.Д. Информационная безопасность как инструмент обеспечения экономической безопасности предприятий / Д.Д. Злыгостев, Р.С. Зарипова / Инновации в информационных технологиях, машиностроении и автотранспорте: Сборник материалов Международной научно-практической конференции. – Кемерово, 2017. – С. 23-25.

3. Ромашкин В.А. Влияние информационных технологий на современное общество / В.А. Ромашкин, О.А. Пырнова, Р.С. Зарипова // Современные научные исследования и разработки. – 2018. – №9(26). – С. 341-344.

4. Хайруллин А.М. Концепция и методы инженерно-технической защиты информации / А.М. Хайруллин, Р.С. Зарипова / Аллея науки. – 2018. – Т.1. – №2(18). – С.290-293.

5. Шакиров А.А. Обеспечение информационной безопасности организаций / А.А. Шакиров, Р.С. Зарипова // Аллея науки. – 2018. – Т.3. – №1(17). – С. 841-843.

6. Шакиров А.А. Актуальность обеспечения информационной безопасности в условиях цифровой экономики / Шакиров А.А., Зарипова Р.С. / Инновационное развитие экономики. Будущее России: Сборник материалов и докладов V Всероссийской (национальной) научно-практической конференции. – 2018. – С. 257-260.